

AO 106 Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of:

12607 W. Vista Paseo Dr., Litchfield Park, AZ 85340
and the person of Christina Marie Chapman.

Case No. 23-6160MB

APPLICATION FOR A SEARCH WARRANT

I, Cody Rehner, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

As further described in Attachment A

located in the District of Arizona, there is now concealed:

As set forth in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code/Section</i>	<i>Offense Description</i>
18 U.S.C. § 1960	Unlicensed Money Transmitting Business
18 U.S.C. § 1324	Bringing in/Harboring Aliens
18 U.S.C. § 1956	Money Laundering

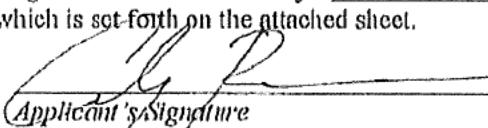
The application is based on these facts:

See attached Affidavit of Special Agent Cody Rehner

☒ Continued on the attached sheet.

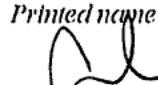
☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA David Plimsner


 Applicant's Signature

Cody Rehner, Special Agent, Federal Bureau of Investigation
 Printed name and title

Sworn to before me telephonically and signed.

Date: October 25, 2023 @ 6:27pm

 Judge's signature
City and state: Phoenix, Arizona

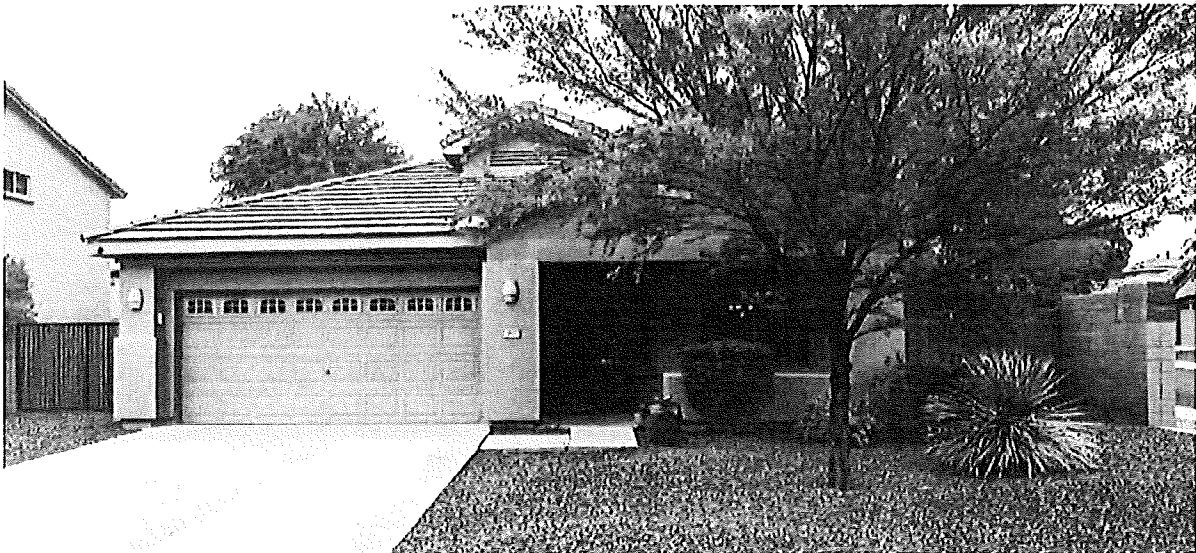
Honorable Alison S. Bachus, U.S. Magistrate Judge
 Printed name and title

ATTACHMENT A

Property to Be Searched

The property and places to be searched are:

- (1) 12607 W Vista Paseo Dr., Litchfield Park, Arizona, 85340. The residence is a one-story, single-family home with a tan and beige stucco exterior, and tile roof. A photograph of the residence is included below.



- (2) The person of Christina Marie Chapman, pictured below, having SSN [REDACTED] 7030 and DOB [REDACTED] 1975.



ATTACHMENT B

Property to be seized

1. All records relating to violations 18 U.S.C. §§ 1956 (laundering of international monetary instruments), 1960 (unlicensed money transmitting business), and 8 U.S.C. § 1324 (unlawful employment of aliens), and occurring in or after January 2021, including:

- a. records and information relating to a conspiracy to defraud entities seeking to employ remote workers;
- b. records and information relating to a conspiracy to launder funds to and from the United State to and from a location outside the United States;
- c. employment records of remote workers and Christina Marie Chapman;
- d. financial records of remote workers and Christina Marie Chapman;
- e. personal identification documents for Christina Marie Chapman;
- f. records and information relating to the location of participants in a scheme to defraud U.S.-based entities seeking to employ remote workers;

- g. records and information relating to **Company 1** **COMPANY 2** **COMPANY 3**

COMPANY 3 **COMPANY 4** **COMPANY 5** **COMPANY 6**

COMPANY 6 **COMPANY 7**

COMPANY 8 **COMPANY 9** **COMPANY 10** **COMPANY 11**

COMPANY 11 **COMPANY 7** **COMPANY 12**

COMPANY 12 **COMPANY 13**

Individual 2 **Individual 5**

Individual 5 **Individual 1** **Individual 3** **Individual 6** **Individual 3** **Individual 8**

Individual 7 Individual 9 Individual 10 Individual 11 Individual 12

Individual 12 PayPal, Payoneer, Dedipath, GitHub, and CashApp;

- h. records and information related to individuals gaining employment as a remote worker;
 - i. records and information related to U.S.-based entities who employed remote workers;
 - j. records and information relating to the scheme to employ remote workers that are found in email accounts: [REDACTED]
[REDACTED] and [REDACTED]
 - k. records and information relating to the identity or location of the remote workers; and
 - l. records and information relating to malicious software.
2. Books, records, receipts, notes, ledgers, invoices, and any other documentation related to the scheme;
3. Notes containing the individual names of such persons, telephone numbers or addresses of associates in the schemes, and any records of accounts receivable, money paid or received, cash or checks received, or intended to be paid;
4. VOIP equipment and service documents;
5. Records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, cashier's checks, check stubs, PayPal, Payoneer, or other electronic money transfer services, check or money order purchase receipts, account statements, and any other records reflecting the receipt, deposit, or transfer of money;
6. United States currency, foreign currency, and receipts or documents regarding purchases of real or personal property;

7. Safe deposit box keys, storage locker keys, safes, and related secure storage devices, and documents relating to the rental or ownership of such units;

8. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises and any vehicles found thereon during the execution of the warrant, including, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, records of real estate transactions, vehicle titles and registration, and vehicle maintenance records;

9. Photographs, including still photos, negatives, slides, videotapes, and films, in particular those showing co-conspirators, criminal associates, U.S. currency, real and personal property;

10. Computers, cellular phones, tablets, and other media storage devices, such as thumb drives, CD-ROMs, DVDs, Blu Ray disks, memory cards, and SIM cards (hereafter referred to collectively as “electronic storage media”);

11. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

12. Any records and information found within the digital contents of any electronic storage media seized from the Subject Premises, including:

- a. all information related to the offenses as described in paragraph 1;
- b. all bank records, checks, credit card bills, account information, or other financial records;
- c. any information recording schedule or travel;
- d. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, correspondence, and phonebooks;
- e. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use,

and events relating to crime under investigation and to the electronic storage media user;

- f. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;
- g. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;
- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;
- i. evidence of the times the electronic storage media were used;
- j. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;
- k. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;
- l. records of or information about Internet Protocol addresses used by the electronic storage media;
- m. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or

other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from “apps,” including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

This warrant authorizes a review of records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Cody Rehrer, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premise known as 12607 W Vista Paseo Dr, (hereinafter “**Subject Premises**”), a/k/a 12607 W Vista Paseo Dr., Litchfield Park, Arizona 85340 and the person of Christina Marie CHAPMAN, as further described in Attachment A, in order to search for and seize the items outlined in Attachment B, which represent evidence, fruits, and/or instrumentalities of the criminal violations further described below.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), currently assigned to the FBI Phoenix Field Office. I have been a Special Agent with the FBI since 2017. Since approximately 2017, I have principally been involved in national security investigations. Specifically, I have been involved in investigations involving counterterrorism and counterintelligence, sanctions violations, and illicit finance. I have received training in the laws and regulations relating to the International Emergency Economic Powers Act (“IEEPA”), pursuant to Title 50, United States Code, Sections 1701 through 1707. Additionally, I have received training in, among other things, criminal investigative techniques, and I have participated in investigations involving the violation of IEEPA, including laundering illegal proceeds, by causing funds to be transferred through U.S. banks for the benefit of prohibited entities. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States. I am also familiar with efforts used by individuals to obfuscate their location and identity

by using the internet, to include the misuse of borrowed, bought, or stolen identification documents and the employment of virtual private servers or networks.

3. The facts in this affidavit come from my personal observations, my training and experience, information obtained from the knowledge and observations of other sworn law enforcement officers, either directly or indirectly through their reports or affidavits, surveillance conducted by law enforcement officers, information provided by witnesses, analysis of public records, analysis of social media information, and analysis of financial records.

4. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for the requested warrant, your Affiant has not set forth all of the relevant facts known to law enforcement officers.

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of, *inter alia*, 18 U.S.C. §§ 1956 (laundering of monetary instruments), 1960 (unlicensed money transmitting business), and 8 U.S.C. § 1324 (unlawful employment of aliens) have been committed by Christina Marie CHAPMAN and other known and unknown coconspirators. There is also probable cause to search the locations described in Attachment A for evidence of these crimes further described in Attachment B.

II. RELEVANT STATUTES

6. Under 18 U.S.C. § 1960, “whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.” The term “‘unlicensed money transmitting business’ means a money transmitting business which affects interstate or foreign commerce in any manner or degree . . . otherwise involves the transportation or

transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity.”¹

7. Under 8 U.S.C. § 1324, it is unlawful for a person or other entity to hire, or to recruit or refer for a fee, for employment in the United States an alien knowing the alien is an unauthorized alien.

8. Under 18 U.S.C. § 1956, it is illegal to, “knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conduct or attempt to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity.” 1956(A)(1)(a). Both 18 U.S.C. § 1960 and 8 U.S.C. § 1324 qualify as “specified unlawful activity” under the statute.

III. BASIS FOR PROBABLE CAUSE

9. The United States is investigating Christina Marie CHAPMAN (hereinafter “CHAPMAN”), as well as identified and unidentified co-conspirators, for a scheme in which persons are fraudulently obtaining employment with U.S.-based companies for monetary gain and illegally using the U.S. financial system in furtherance of the same. The investigation has revealed that CHAPMAN is knowingly facilitating the fraudulent scheme by lending her U.S.-based address and financial account information to non-U.S. persons overseas who are seeking pseudonymous employment with U.S. companies. In turn, CHAPMAN’s co-conspirators are using CHAPMAN’s residential location and financial accounts to collect payment from U.S. companies

¹ Title 6, Arizona Revised Statutes, 1207 mandates a license in the State of Arizona in order to operate as a money transmitting service. *See* 18 U.S.C. § 1960 (b)(1)(A).

and funneling those funds overseas, all in violation of 18 U.S.C. §§ 1956, 1960, and 8 U.S.C. § 1324.

A. The Subject Premises

10. According to records held within the Maricopa County Assessor's Office, on or about September 29, 2022, the **Subject Premises** was purchased by [REDACTED] from The [REDACTED] dated July 31, 2015, for \$460,000.00 cash. Additionally, the records revealed it was listed as a rental property.

11. At various times from October 4 to October 10, 2023, your Affiant conducted physical surveillance of the **Subject Premises**. Your Affiant observed a Honda Odyssey Van, bearing Minnesota license plate [REDACTED] parked in the driveway. Record checks on this license plate revealed it was last registered to [REDACTED] [REDACTED]

12. Based on a review of CHAPMAN's personal bank account, her transactional patterns shifted from Minnesota based transactions to Arizona based transactions in or around the end of October 2022. CHAPMAN's personal banking information show charges consistent with CHAPMAN renting a U-Haul in Minnesota in or about October 24, 2022, and dropping it off at a U-Haul location in Arizona in or around November 1, 2022.

13. Financial records from two U.S. financial institutions showed that CHAPMAN had listed the **Subject Premises** as her residence with both institutions.

14. The aforementioned surveillance showed no evidence of any other individuals residing at the **Subject Premises**. Additionally, the surveillance showed no evidence of overnight guests at the **Subject Premises**.

15. On or about June 6, 2023, CHAPMAN posted a video to her TikTok account, [REDACTED] [REDACTED], which appeared to be taken at the **Subject Premises** based on the view of the home.

The TikTok video appears to be taken on a cellular phone, based on the movement of the camera during the video. The video showed roughly more than ten laptops that appeared to be running. As described further herein, based on the evidence and information obtained in the investigation to date, each of these laptops represent a different company CHAPMAN was enabling these remote IT workers to be employed with and generate revenue from.

B. Remote Work Scheme

16. The investigation has revealed that CHAPMAN has been involved in a scheme since at least January 2021 as the residential address for remote work employees, despite that there is no evidence that these employees so reside at her address or are even located in the United States. In or around October 2022, CHAPMAN moved from Minnesota to the **Subject Premises**, where she continued the scheme.

Company 1

17. According to information obtained during the course of the investigation, in October 2022, **Company 1** (**COMPANY 1**) a U.S. company, hired a remote IT employee known as **Individual 1**. **Individual 1** Records of **Company 1** confirmed **Individual 1** provided his home address as the **Subject Premises**. Thao also sent documentation verifying his residence as the **Subject Premises** and requested the payroll checks be sent to the **Subject Premises**.

18. According to information provided by **COMPANY 1** during **Individual 1** employment, **COMPANY 1** sent a paper check to **Individual 1** at the **Subject Premises**. Thao reported to **COMPANY 1** that he experienced a problem with the direct deposit, at which point **Company 1** requested **Individual 1** send a picture of the check sent to the **Subject Premises**,

with "VOID" written across it **Individual 1** or someone working with **Individual 1** complied with and so sent the voided check.

19. **Company 1** fired **Individual 1** in or around September 2023 after being contacted by the FBI and conducting an internal review of **Individual 1** records.

Company 2 Employee

20. According to information obtained during the course of the investigation, **Company 2** also known as **Company 2**, a U.S. company, hired a remote IT employee named **Individual 1** which fit a similar profile to the **Company 2** employee. **Company 2** confirmed **Individual 1** address on file was the **Subject Premises** and that the **Subject Premises** was used on all **Individual 1** payroll and tax documents.

Company 3 Employee

21. According to information obtained during the course of the investigation, in May 2023, The **Company 3** Insurance Company, also known as **Company 3** **Company 3** a U.S. company, hired a remote IT worker known as **Individual 2**. **Individual 2** stated his address was **Individual 2** Las Vegas, NV 89121, however **Individual 2** stated that while he was "recovering from surgery," he was working from "his parents address," the **Subject Premises**. **Individual 2** requested **Company 3** to ship their company laptop to the **Subject Premises** for **Individual 2** to start the remote work. **Individual 2** also provided **Company 3** with Voice over Internet Protocol ("VOIP") number **Individual 2** and email address **Individual 2** as methods of contact.

22. On or about May 8, 2023, **Individual 2** officially started work with **Company 3** and shortly after **Individual 2** beginning orientation, **Company 3** Security Operation Center (hereinafter

“SOC”), which was responsible for protecting their organization from cyber threats, was notified that Individual 2 attempted to download AnyDesk² on his company provided laptop.

23. On May 8, 2023, a network log showed Individual 2 Company 3 computer attempted to access a site associated with Remote Access software, anydesk.com. Approximately 38 minutes later, Individual 2 Company 3 computer accessed a Company 3 network resource from a suspicious Internet Service Provider (ISP) by attempting to login from source IP [REDACTED].202, with a machine using the Linux operating system. Company 3 SOC determined that this login request originated from an organization called Colocrossing, colocrossing.com, from the city of Victoria in the country of Seychelles. According to Colocrossing’s website, it provides top quality virtual private servers (VPS) solutions to its customers. Based on my training and experience, a virtual private server is a virtual machine that provides a virtualized server resources on a physical server that is shared with other uses. VPS hosting allows users to get dedicated server space with a reserved amount of resources, while offering them greater control and customization than shared hosting, essentially a server that is rented to host another server.

24. Company 3 SOC blocked the download, turned on the laptop’s camera. The camera captured a screenshot of CHAPMAN. Company 3 immediately terminated Individual 2 employment contract.

//

² AnyDesk is a remote desktop application distributed by AnyDesk Software GmbH. The proprietary software program provides a platform independent remote access to personal computers and other devices running the host application. It offers remote control, file transfer, and VPN functionality. According to <https://aura.com>, “AnyDesk is a legitimate software tool that allows people to remotely view and control computers and mobile devices. For example, if an employee at a large company has a technical issue, someone on the IT team can use AnyDesk to “take over” the device and diagnose the problem.”

Other Employees of U.S. Companies

25. A review of CHAPMAN's bank account at a Wells Fargo suggests that CHAPMAN's scheme extends to many other U.S. employers. According to records of CHAPMAN's account, CHAPMAN deposited the following checks into her account, most of which were payroll checks. All the checks were deposited after the purported beneficiary of the check signed the check over to CHAPMAN and CHAPMAN had signed the check for deposit. Bank statements from Wells Fargo stated that these deposits were all "Mobile Deposits," which, according to Wells Fargo's website, means that CHAPMAN used her cellular phone to take pictures of the checks that she received for these individuals for deposit into her account.

U.S. Company	Pay To Order	Date of Check	Amount	Date of Deposit	Address
Company 4	Individual 3	9/15/2022	\$ 3,328.58	9/27/2022	None
Company 4	Individual 3	9/15/2022	\$ 4,886.26	9/30/2022	None
Company 4	Individual 3	9/30/2022	\$ 4,886.27	10/11/2022	None
Company 5	Individual 2	1/27/2023	\$ 2,367.34	3/6/2023	██████████ Las Vegas, NV 89121
Company 6	Individual 6	2/9/2023	\$ 4,175.23	3/24/2023	CHAPMAN's Residence in MN
Company 7	Individual 7	3/15/2023	\$ 3,840.17	3/28/2023	Subject Premises
Company 7	Individual 7	3/31/2023	\$ 3,840.08	4/12/2023	None
Company 8	Individual 3	4/3/2023	\$ 2,179.53	4/25/2023	None
Company 9	Individual 8	3/6/2023	\$ 4,551.65	5/1/2023	Subject Premises
Company 10	Individual 10	4/11/2023	\$ 4,379.36	5/17/2023	Subject Premises

Company 7	Individual 7	5/15/2023	\$ 3,840.17	5/19/2023	Subject Premises
Company 7	Individual 7	4/13/2023	\$ 3,899.65	6/7/2023	Subject Premises
Company 11	Individual 9	2/28/2023	\$ 960.44	6/12/2023	FL Address
Company 7	Individual 7	5/31/2023	\$ 3,840.09	6/20/2023	None
Company 10	Individual 10	6/16/2023	\$ 4,713.87	7/6/2023	Subject Premises
Company 12	Individual 11	7/20/2023	\$ 3,264.00	8/3/2023	MN Address
Company 13	Individual 12	6/27/2023	\$ 2,318.19	8/14/2023	Subject Premises

26. Records from Wells Fargo further show that CHAPMAN operated as a money transmitter, sending some of these funds out shortly after receiving them. For instance, with respect to the first three payments to **Individual 3** CHAPMAN caused wire transactions to be sent from her Wells Fargo account to an individual named **Individual 4** in New York, a few days after the checks were deposited. Two of the three checks and wires match exactly, while the first check to wire shows that CHAPMAN may have taken a commission (\$2800) for her services, as follows:

- a. 9/28/2022 - \$544
- b. 10/3/2022 - \$4856.26
- c. 10/14/2022 - \$4856.27

27. CHAPMAN made regular withdrawals from her accounts and often sent thousand dollar payments to other financial institutions, including, for instance, Wise, a U.K. based financial services provider.

28. Between January 1, 2021, and August 15, 2023, CHAPMAN's Wells Fargo bank account had inflows totaling \$267,640 and outflows of \$237,006 with an ending balance on August 15, 2023, of \$30,634.

29. Thus, there is probable cause to believe that CHAPMAN was utilizing her residence as the home address for remote employees, who had submitted false information to their employer regarding their identities, and that CHAPMAN was using her bank account to move proceeds of the scheme.

C. CHAPMAN's Additional Financial Transactions

Payoneer Accounts

30. CHAPMAN was the account holder of three accounts at Payoneer. According to Payoneer's website, Payoneer is an American financial services company that provides online money transfer, digital payment services, and provides customers with working capital.

31. Business records from Payoneer show that CHAPMAN received approximately \$45,230 of transfers into her accounts at Payoneer between February 28, 2022, and July 11, 2022. The majority of these transfers were from Individuals located in China, near the North Korean border.

32. The individual that remitted the largest amount of funds to CHAPMAN was Individual 5. Individual 5 sent Chapman ten transfers totaling approximately \$26,289.40 between February 28, 2022, and June 3, 2022, all of which originated from China. CHAPMAN transferred these Payoneer funds to a bank account in her name at Capital One.

33. A review of Chapman's Capital One checking account ending 6710 showed that CHAPMAN received these Payoneer funds into that account and also revealed that CHAPMAN received funds into this account from multiple sources. One of these sources of incoming funds was from a company named **Company 14**

34. Open-source information shows that **Company 14** is a mobile app development company. Funds deposited into CHAPMAN's account by **Company 14** were set up on a direct deposit basis and occurred on a bi-weekly basis similar to payments received for employment. Whenever CHAPMAN received a payment from **Company 14** there was a corresponding transfer from the Capital One bank account ending 6710 to Payoneer. These transfers are summarized below:

Capital One Company 14 Deposit Date	Capital One Company 14 Deposit Amount	Capital One Transfer to Payoneer Date	Capital One Transfer to Payoneer Amount
05/19/2022	\$8,662.14	05/24/2022	\$8,662.14
06/02/2022	\$4,331.12	06/06/2022	\$4,331.12
06/16/2022	\$4,331.14	06/21/2022	\$4,331.14
06/30/2022	\$4,331.12	07/06/2022	\$4,331.00
07/14/2022	\$4,331.14	07/18/2022	\$4,330.00
Total	\$25,986.66	Total	\$25,985.40

35. These five payments received from **Company 14** are the only payments received from this entity by CHAPMAN's Capital One account ending 6710. Payoneer documentation showed that these five transfers were sent from CHAPMAN to **Individuals**. The relationship between the funds received from **Individual** and the funds sent to **Individual** are unknown at this time.

36. CHAPMAN knowingly received this money from a company through direct deposit for an individual not legally authorized to obtain work within the U.S. CHAPMAN intentionally redirected these funds to her personal Payoneer account to then transmit these funds **Individual 5** who received them in China, near the North Korean border.

37. There appeared to be little to no profit being kept for CHAPMAN as she was primarily moving the total amount received from **Company 14** to separate Payoneer accounts in order to layer the transactions. These funds ultimately left Payoneer via withdrawals from bank accounts located in China, near the North Korean border. Based on my training and experience, this movement of funds was indicative of mule accounts operating together to move funds from one location to another without any clear legitimate purpose and to launder the funds to a high-risk jurisdiction. CHAPMAN was functioning as a money transmitting business with no license by the transmission of funds on behalf of **Individual 5** from the United States to abroad by electronic transfer.

38. According to business records of Payoneer, CHAPMAN recorded her mobile telephone number as **8497** and email addresses as **CHAPMAN's** Payoneer account revealed the Payoneer mobile application (*i.e.*, utilized by CHAPMAN's mobile cellular phone) was utilized multiple times to login to her accounts from locations in the United States and also locations other than the United States, which is consistent with the illegitimate movement of funds.

- a. A review of CHAPMAN's Capital One account revealed on or about April 20, 2022, CHAPMAN performed a mobile check deposit in the amount of \$1,751.60. Then on or about April 29, 2022, Capital One processed a withdrawal to CHAPMAN's Payoneer account in the amount of \$1,750.84. Records obtained

from Payoneer showed on or about April 28, 2022, CHAPMAN performed an international U.S. dollar transfer through Payoneer to an account located in China owned by [REDACTED] for \$1,750.84. Further analysis of CHAPMAN's login data revealed CHAPMAN logged into her Payoneer account on or about April 28, 2022, utilizing an IP address geolocated to Minneapolis, Minnesota from Comcast Cable internet service provider utilizing an Android device, a cellular phone device. Immediately after logging into her account, CHAPMAN performed a "CardToGBTransfer." This was the only outbound transfer action that occurred on the same date as the \$1,750.84 U.S. dollar transfer to [REDACTED] account in China.

- b. Additionally, this login data also showed her account was logged into on or about July 3, 2022, by device ID [REDACTED] C1E57 (hereinafter "Dandong Device ID"), from IP address [REDACTED] out of Dandong, China. This IP address was owned by China Unicom. This device ID was different from the one used by CHAPMAN to register for and to make changes to her Payoneer accounts. Based on Payoneer's multifactor-authentication requirements for their account holders, CHAPMAN would have to be in direct contact with the user who logged into her account from the Dandong, China IP address in order to provide them the verification code to allow a successful login. Although this was not the first instance of Dandong Device ID successfully logging into CHAPMAN's Payoneer account, it was the only time the device did not utilize an anonymization service to obfuscate its true location.

- c. On or about July 5, 2022, the next time Dandong Device ID logged into CHAPMAN's account they reverted back to utilizing DediPath³ to show their IP address as coming from Los Angeles, California. Utilization of a VPN or VPS service is consistent with the scheme of alien remote workers attempting to maintain the anonymity of telework arrangements they require to operate.

39. CHAPMAN's Capital One bank accounts, referenced earlier in this section, had inflowing funds totaling \$346,997 and outflowing funds totaling \$346,808 between January 1, 2021, and July 31, 2023, leaving a balance of approximately \$189 as of July 31, 2023.

CHAPMAN's PayPal Accounts

40. CHAPMAN owns several accounts at PayPal, but only actively uses roughly four accounts. One of these accounts (hereinafter "PayPal Account 1"), had deposits of U.S. dollars totaling roughly \$200,000, with a similar amount leaving the account, between January 2021 and August 2023. Of the deposited funds, CHAPMAN received 90 transfers totaling approximately \$142,919 between March 2021 and March 2023 from [REDACTED] Individual 5 PayPal account ending 3648. Most of the transfers contained notes that referenced "Service Fee", "Shipment Fee", "Development Work", "Web Design", "Purchase Computer", "Equipment Purchase", "HTML Design", etc. Between September 2021 and June 2023, CHAPMAN withdrew \$153,857 from PayPal Account 1 and sent these funds to her Capital One bank account.

³ As of August 31, 2023, DediPath abruptly shut down, giving their customers less than 24 hours notice. Upon review of their historical website, <https://web.archive.org/web/20230831122307/https://dedipath.com/about-us>, DediPath stated their services were to provide infrastructure as a service (IaaS), managed services, and colocation, including VPN/VPS services.

41. Records related to Individual 5 PayPal account ending 3648 showed the account was created on September 5, 2016, by an individual named Individual 5 which is Chinese for Individual 5. Individual 5 listed an address in Dandong, China that is less than one mile from the North Korea border. Individual 5 listed that he worked in "Computer Hardware and Software." Individual 5 attached nine different Chinese bank accounts to his PayPal account between July 2018 and July 2022 to include accounts at Zhenjian Chouzhou Commercial Bank, Industrial Bank, Industrial and Commercial Bank of China, Bank of China and China Construction Bank. Individual 5 account received roughly \$790,500 between January 2021 and April 2023.

42. On or around September 2, 2022, Xu's PayPal account ending 3648 had a U.S. dollar payment for \$33. The transaction was labeled an "Automatic fund deposit" and included and invoice number of "ppfund-kouthao0-3154a67ce45161d9". The inclusion of the name Individual 1 in this invoice number would suggest that this payment was related to work performed by Individual 1. The counterparty of the transaction was serverpoint.com which is a company that hosts websites and offers website development tools located in Las Vegas, Nevada.

43. According to business records provided by PayPal, CHAPMAN was also the owner of another PayPal account (hereinafter "PayPal Account 2"). PayPal Account 2 was utilized to pay for a national criminal and offense report from SentryLink LLC⁴ for approximately 17 different individuals from March through August of 2023. This same account was also used to pay for social security number traces for approximately 21 different individuals from March through

⁴ SentryLink LLC is a Maryland based background screening service with more than a decade of experience in job applicant screening and general background check services. The company focuses on criminal background and driving records. SentryLink covers the majority of the United States along with the US Virgin Islands, Puerto Rico, and Guam.

August 2023. (Records of CHAPMAN's Wells Fargo debit card also showed transactions with Sentry Link in 2023.)

44. According to SentryLink LLC's website, their national criminal and offense report is a comprehensive criminal check showing felonies, misdemeanors, sex offenses and more at the state and county level. According to SentryLink LLC's website, their social security number trace report validates a social security number, finds maiden names and middle names, and checks the death master index. It also shows all names associated with this SSN and list previous counties of residence for deeper background checks.

Money Service Business Registration Records

45. A review of the Department of Treasury, FinCEN's online money service business registration website, <https://www.fincen.gov/msb-state-selector>, revealed no licensed business known to be associated with CHAPMAN.

46. A review of the Arizona Department of Economic Security records revealed no records for claims, wages, and/or benefits filed under CHAPMAN's social security number over the last three years.

47. A review of the Arizona Corporation Commission records revealed no records of an established entity associated with CHAPMAN.

48. A review of the Office of the Minnesota Secretary of State revealed no records of an established entity associated with CHAPMAN.

IV. ITEMS TO BE SEIZED

49. Based upon the facts contained in this Affidavit, your Affiant submits there is probable cause to believe that the items listed in Attachment B will be found at the **Subject Premises**.

50. Based on my training, education, and experience, and discussions with other trained law enforcement personnel, along with information provided by sources of information and confidential sources, your Affiant knows the following:

51. Individuals involved in money laundering schemes often maintain paper records of their money laundering activities. Your Affiant knows that such records are commonly maintained for long periods of time and therefore are likely to be found at the **Subject Premises**.

52. Individuals involved in money laundering schemes commonly use computers, cellular phones, and other electronic devices to communicate with other conspirators about the scheme through the use of telephone calls, text messages, email, chat rooms, social media, and other internet- and application-based communication forums. Moreover, such individuals commonly use other capabilities of computers and electronic devices to further their money laundering activities. Therefore, evidence related to money laundering activity is likely to be found on electronic storage media found at the **Subject Premises**, as further described below.

53. In my training and experience, people typically store their electronics and correspondence (including letters or printed emails) in their homes and transport them in their vehicles. I also know that people typically carry small electronic storage devices and communication devices, such as cellular phones, flash drives, and thumb drives, on their person.

54. In addition to items which may constitute evidence, fruits and/or instrumentalities of the crimes set forth in this Affidavit, your Affiant also requests permission to seize any articles tending to establish the identity of persons who have dominion and control over the **Subject Premises**, including rent receipts, utility bills, telephone bills, addressed mail, personal identification, keys, purchase receipts, sale receipts, photographs, vehicle pink slips, and vehicle registration.

V. DIGITAL EVIDENCE STORED WITHIN ELECTONRIC STORAGE MEDIA

55. As described in Attachment B, this application seeks permission to search for records that might be found in or on the **Subject Premises**, in whatever form they are found, including data stored on a computer, cellular phone, tablet, or other media storage device, such as a thumb drive, CD-ROM, DVD, Blu Ray disk, memory card, or SIM card (hereafter collectively referred to as “electronic storage media”). Thus, the warrant applied for would authorize the seizure of all electronic storage media found in or on the **Subject Premises** and, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

56. *Probable cause.* Your Affiant submits that if electronic storage media are found in or on the **Subject Premises**, there is probable cause to believe records and information relevant to the criminal violations set forth in this Affidavit will be stored on such media, for at least the following reasons:

- a. Your Affiant knows that when an individual uses certain electronic storage media, the electronic storage media may serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage media is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic storage media is also likely to be

a storage medium for evidence of crime. From my training and experience, your Affiant believes that electronic storage media used to commit a crime of this type may contain: data that is evidence of how the electronic storage media was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

- b. Based on my knowledge, training, and experience, your Affiant knows that electronic storage media contain electronically stored data, including, but not limited to, records related to communications made to or from the electronic storage media, such as the associated telephone numbers or account identifiers, the dates and times of the communications, and the content of stored text messages, e-mails, and other communications; names and telephone numbers stored in electronic “address books;” photographs, videos, and audio files; stored dates, appointments, and other information on personal calendars; notes, documents, or text files; information that has been accessed and downloaded from the Internet; and global positioning system (“GPS”) information.
- c. Based on my knowledge, training, and experience, your Affiant knows that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on an electronic storage medium, the data contained in the

file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- e. As previously set forth in this Affidavit, the targets of this investigation have used computers to execute their fraudulent scheme, including to allow individuals located overseas to log onto U.S. businesses’ networks. Therefore, your Affiant believes that evidence of criminal activity will be found on any electronic storage media found at the **Subject Premises** and that the electronic storage media constitute instrumentalities of the criminal activity.

57. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be found on any electronic storage media located in or on the **Subject Premises** because:

- a. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that

show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. File systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within electronic storage medium (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the owner. Further, activity on an electronic storage

medium can indicate how and when the storage medium was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on an electronic storage medium may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the existence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera) not previously identified. The geographic and timeline information described herein may either inculcate or exculpate the user of the electronic storage medium. Last, information stored within an electronic storage medium may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information within a computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping"

program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic storage medium evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on one electronic storage medium is evidence may depend on other information stored on that or other storage media and the application of knowledge about how electronic storage media behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how an electronic storage medium was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

58. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a **Subject Premises** for information that might be stored on electronic storage media often requires the seizure of the physical storage media and later off-site review consistent

with the warrant. In lieu of removing storage media from the **Subject Premises**, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on **Subject Premises** could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine electronic storage media to obtain evidence. Electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the **Subject Premises**. However, taking the electronic storage media off-site and reviewing it

in a controlled environment allows for a thorough examination with the proper tools and knowledge.

- c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats that may require off-site reviewing with specialized forensic tools.

59. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant your Affiant is applying for would permit seizing, imaging, or otherwise copying electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

//

//

//

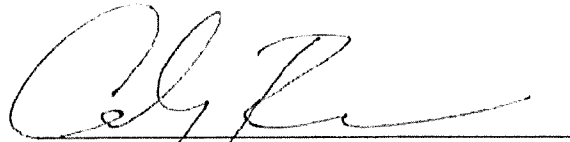
//

//

//

CONCLUSION

61. Your Affiant submits there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 1956 (laundering of monetary instruments), 1960 (unlicensed money transmitting business), and 8 U.S.C. § 1324 (unlawful employment of aliens) are likely to be found at the **Subject Premises** and on the person of Christina Marie CHAPMAN which is further described in Attachment A.



Cody Rehner
Special Agent
Federal Bureau of Investigation

Telephonically subscribed and sworn to before me on this 25th day of October, 2023.



HONORABLE ALISON S. BACHUS
United States Magistrate Judge

AO93 Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of:

12607 W. Vista Paseo Dr., Litchfield Park, AZ 85340
and the person of Christina Marie Chapman.

Case No. 23-6160MB

(Filed Under Seal)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona:

As further described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

As set forth in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before November 8, 2023 *(not to exceed 14 days)*
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the District of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized ☐ for 30 days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: October 25, 2023@6:30pm


Judge's signature

City and state: Phoenix, Arizona

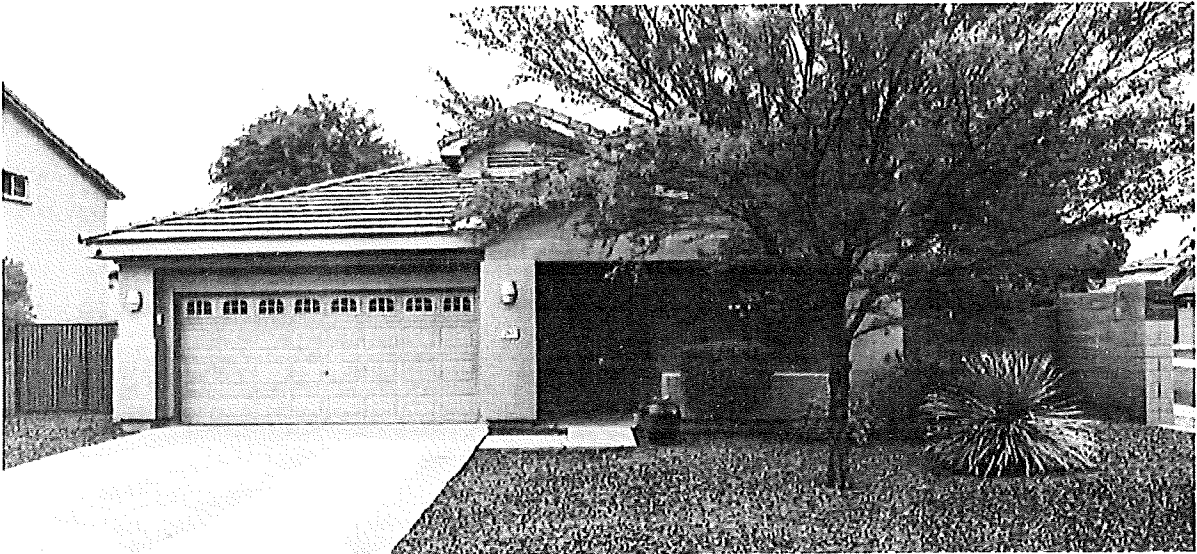
Honorable Alison S. Bachus, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The property and places to be searched are:

- (1) 12607 W Vista Pasco Dr., Litchfield Park, Arizona, 85340. The residence is a one-story, single-family home with a tan and beige stucco exterior, and tile roof. A photograph of the residence is included below.



- (2) The person of Christina Marie Chapman, pictured below, having SSN [REDACTED] 7030 and DOB [REDACTED] 975.



ATTACHMENT B

Property to be seized

1. All records relating to violations 18 U.S.C. §§ 1956 (laundering of international monetary instruments), 1960 (unlicensed money transmitting business), and 8 U.S.C. § 1324 (unlawful employment of aliens), and occurring in or after January 2021, including:

- a. records and information relating to a conspiracy to defraud entities seeking to employ remote workers;
- b. records and information relating to a conspiracy to launder funds to and from the United State to and from a location outside the United States;
- c. employment records of remote workers and Christina Marie Chapman;
- d. financial records of remote workers and Christina Marie Chapman;
- e. personal identification documents for Christina Marie Chapman;
- f. records and information relating to the location of participants in a scheme to defraud U.S.-based entities seeking to employ remote workers;

g. records and information relating to **Company 1** **COMPANY 2** **COMPANY 3**

COMPANY 3 **COMPANY 4** **COMPANY 5** **COMPANY 6**

COMPANY 6 **COMPANY 7**

COMPANY 8 **COMPANY 9** **COMPANY 10** **COMPANY 11**

COMPANY 11 **COMPANY 7** **COMPANY 12**

COMPANY 12 **COMPANY 13**

Individual 2 **Individual 5**
Capital One Financial, Wells Fargo,

Individual 5 **Individual 1** **Individual 3** **Individual 6** **Individual 3** **Individual 8**

Individual 7 Individual 9 Individual 10 Individual 11 Individual 12

Individual 12 PayPal, Payoneer, Dedipath, GitHub, and CashApp;

- h. records and information related to individuals gaining employment as a remote worker;
 - i. records and information related to U.S.-based entities who employed remote workers;
 - j. records and information relating to the scheme to employ remote workers that are found in email accounts: [REDACTED]
[REDACTED] and [REDACTED]
 - k. records and information relating to the identity or location of the remote workers; and
 - l. records and information relating to malicious software.
2. Books, records, receipts, notes, ledgers, invoices, and any other documentation related to the scheme;
3. Notes containing the individual names of such persons, telephone numbers or addresses of associates in the schemes, and any records of accounts receivable, money paid or received, cash or checks received, or intended to be paid;
4. VOIP equipment and service documents;
5. Records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, cashier's checks, check stubs, PayPal, Payoneer, or other electronic money transfer services, check or money order purchase receipts, account statements, and any other records reflecting the receipt, deposit, or transfer of money;
6. United States currency, foreign currency, and receipts or documents regarding purchases of real or personal property;

7. Safe deposit box keys, storage locker keys, safes, and related secure storage devices, and documents relating to the rental or ownership of such units;

8. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises and any vehicles found thereon during the execution of the warrant, including, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, records of real estate transactions, vehicle titles and registration, and vehicle maintenance records;

9. Photographs, including still photos, negatives, slides, videotapes, and films, in particular those showing co-conspirators, criminal associates, U.S. currency, real and personal property;

10. Computers, cellular phones, tablets, and other media storage devices, such as thumb drives, CD-ROMs, DVDs, Blu Ray disks, memory cards, and SIM cards (hereafter referred to collectively as “electronic storage media”);

11. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

12. Any records and information found within the digital contents of any electronic storage media seized from the Subject Premises, including:

- a. all information related to the offenses as described in paragraph 1;
- b. all bank records, checks, credit card bills, account information, or other financial records;
- c. any information recording schedule or travel;
- d. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, correspondence, and phonebooks;
- e. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use,

and events relating to crime under investigation and to the electronic storage media user;

- f. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;
- g. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;
- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;
- i. evidence of the times the electronic storage media were used;
- j. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;
- k. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;
- l. records of or information about Internet Protocol addresses used by the electronic storage media;
- m. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or

other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from “apps,” including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

This warrant authorizes a review of records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.